UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

CHRISTINE RIGANIAN, et al.,

Plaintiffs,

v.

LIVERAMP HOLDINGS, INC., et al.,

Defendants.

Case No. 25-cv-00824-JST

ORDER GRANTING IN PART AND DENYING IN PART MOTION TO DISMISS

Re: ECF No. 49

Before the Court is Defendants LiveRamp Holdings, Inc. and LiveRamp, Inc.'s (together, "Defendants") motion to dismiss. The Court will grant the motion in part and deny it in part.

I. BACKGROUND[1]

Plaintiffs Christina Riganian and Donna Spurgeon bring this action on behalf of themselves and multiple proposed classes against LiveRamp Holdings, Inc. and LiveRamp, Inc. ("LiveRamp"). Plaintiffs allege that despite them never having directly interacted with LiveRamp, LiveRamp has tracked, compiled, and analyzed vast quantities of their personal, online, and offline activities to build detailed "identity profiles" on them for sale to third parties. ECF No. 32 ¶¶ 1–9, 13–38.

According to Plaintiffs, LiveRamp's is a registered "data broker" in California, which is defined as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." *Id.* ¶ 51 (quoting Cal. Civ. Code § 1798.99.80). LiveRamp has built its business around facilitating a commercial

[1] For the purpose of resolving the motion to dismiss, the Court accepts as true the allegations in the first amended complaint, ECF No. 32 ("FAC"). *Knievel v. ESPN*, 393 F.3d 1068, 1072 (9th Cir. 2005).

surveillance ecosystem in which it connects what third parties know about consumers with the places where consumers may be found. *Id.* ¶ 52. LiveRamp does so as follows: First, it collects and purchases massive amounts of disparate and "virtually unassociated" personal information from countless sources both offline and online, including names, addresses, phone numbers, digital and device identifiers. *Id.* ¶¶ 3, 114. Then, it synchronizes that aggregated data into a single "identity profile" for commercial use, with each individual associated with a unique "RampID" profile that tracks individuals across devices and offline contexts. *Id.* ¶¶ 6, 70–73, 114. Finally, LiveRamp operates a Data Marketplace ecosystem where advertisers and other data brokers can buy and sell information relating to the data compiled in these RampID Profiles. *Id.* ¶¶ 7, 14, 114, 118.

LiveRamp "maintains the largest and most accurate people-based identity graph on the market, purportedly containing detailed personal information on 700 million consumers globally." *Id.* ¶ 6 (internal quotation omitted). It "claims to have 'resolved' the identities of more than 250 million consumers in the United States (*i.e.*, virtually every single adult) 'and many more worldwide' by assigning them each a unique RampID." *Id.* ¶ 59 (footnote omitted).

A. LiveRamp's Alleged Data Collection

LiveRamp's massive data accumulation is powered by both its own surveillance technologies and partnerships with hundreds of third-party data sources. LiveRamp collects personal data through several avenues, including:

(1) internet "cookies," which are placed on users' devices to track web browsing and connect activity to a RampID, *id.* ¶¶ 74–76;

(2) "client-side tags" deployed via "tracking pixels" that automatically capture the website browsing history of individuals matched to their specific RampIDs, *id.* ¶ 78;

(3) Authenticated Traffic Solutions ("ATS") JavaScript Code and Software Development Kit ("SDK"), which allow LiveRamp to detect through "event listeners" the input of personal information, such as email addresses and phone numbers, communicated by consumers to LiveRamp's partner websites, and which—according to LiveRamp—have been adopted by over 21,000 publisher domains, allowing LiveRamp to connect to over 92% of U.S. consumer time

spent online, *id.* ¶ 79; and

(4) the AbiliTec system, which "combines common matching techniques—such as probabilistic matching, approximate string matching, and other typical matching approaches . . . with comparison of customer data to a vast multi-sourced historical repository of consumer contact information to identify individual consumers and assign them each a single AbiliTec ID"—which are constructed from hundreds of sources containing "offline" identifiers such as names, phone numbers, postal addresses, social security numbers, and driver's license records, all of which follow "people across time and space as they change names (due to marriage, divorce, gender transition, or for other reasons) and residences," *id.* ¶¶ 64–68.

B. RampID and Identity Resolution

LiveRamp uses its RampID Identity Graph and AbiliTec ID system to aggregate and synchronize the collected information to perform what it calls "identity resolution." This process involves: (1) combining all available offline identifiers and online tracking signals to build a single, unique "RampID" profile for each individual; and (2) updating and maintaining these profiles "in real time" as individuals move between websites, apps, physical stores, and devices. *Id.* ¶¶ 6, 64–72, 90. Through its identity resolution process, LiveRamp maintains highly detailed, continuously updated dossiers on hundreds of millions of people, which function as a private population registry with a unique ID attached to each real-world identity. *Id.* ¶ 3.

C. The Data Marketplace

LiveRamp monetizes its RampID product through its Data Marketplace—a central exchange where LiveRamp and its clients, many of which are AdTech companies, sell or share access to segments built from the RampID identity graph. *Id.* ¶¶ 54, 85. The Data Marketplace contains segments based on both standard demographics and sensitive attributes—such as health conditions, financial vulnerability, religious affiliation, and sexual orientation. *Id.* ¶¶ 7, 28, 60, 94–107. For example, the FAC alleges that through the Data Marketplace, "LiveRamp's clients bought and sold 'segments' of digital identifiers associated with people with cancer, union members, Muslims, Jewish people, African Americans, poor people, payday loan prospects, online gamblers, unemployed individuals who were 'seen at clinics/hospitals' and users of the LGBT

dating app Grindr." *Id.* ¶ 97. While "LiveRamp claims to prohibit putting certain sensitive segment data up for sale on the Marketplace," the FAC alleges that "it is impossible to tell whether and how LiveRamp enforces these restrictions. For example, the policy claims to prohibit segments relating to reproductive health and rights, pregnancy, and fertility, but in reality vast amounts of records are for sale on the Marketplace that target pregnancy and interest in pregnancy." *Id.* ¶ 100 (internal footnotes and quotations omitted).

Additionally, through its "Third-Party Attribute Enrichment" feature, LiveRamp offers for sale through the Data Marketplace access to all available data seller attributes for individual consumers of interest. *Id.* ¶ 108. For example, LiveRamp's customers can provide non-anonymized, first-party data (such as names, physical addresses and email addresses) and buy the segment data of their choice (including details about their occupation, health, relationship status, finances, and shopping habits) that is associated with that person. *Id.* ¶¶ 108–10. Together with LiveRamp's comprehensive data collection and identity resolution, this enables LiveRamp's customers to target consumers "on an individual level wherever they (or their devices) may be found online or offline)." *Id.* ¶ 112.

D. Plaintiffs

Plaintiff Christina Riganian is a resident of Tujunga, California. *Id.* ¶ 13. Upon filing a "Subject Access Request" ("SAR") with LiveRamp, Riganian received her SAR file revealing that LiveRamp had compiled decades of offline data such as her name, postal address history, and phone numbers that LiveRamp linked to online identifiers like cookies, device IDs, and smart TV IDs. *Id.* ¶¶ 14, 15. Riganian specifically alleges that she interacted with the CVS pharmacy website multiple times to "view information on specific conditions and medications," and that during these visits, LiveRamp's tracking technologies captured full string URLs and other communications reflecting her activity on the CVS site. *Id.* ¶¶ 22–26.

Plaintiff Donna Spurgeon is a resident of Lowell, Oregon, who likewise received her SAR file detailing the identity profile associated with her RampID. *Id.* ¶¶ 29, 30. Spurgeon also claims that her profile contains extensive personal information spanning many years, combined and resolved into a single RampID that connects identifiers linked with her devices, browsers, and

physical addresses. *Id.* ¶ 30. Spurgeon alleges that her activity on at least the following websites were tracked by LiveRamp: healthline.com; CVS.com; Abcnews.go.com; Patient.info; Svu.edu; Health.usnews.com; and Showtime.com. *Id.* ¶ 37. She claims that LiveRamp's tracking technologies captured and transmitted information conveyed in these interactions—including the "precise articles read, products viewed, and searches queried"—to add to her RampID profile. *Id.* ¶ 36.

Plaintiffs allege that they—and the hundreds of millions of people LiveRamp profiles—never meaningfully consented to this pervasive surveillance because they "cannot reasonably foresee all the ways in which LiveRamp may use the comprehensive identity profiles it is compiling on them" or all "the specific third parties to which LiveRamp will provide their personal information or what those third parties will do with that information." *Id.* ¶ 154.

Plaintiffs assert six claims for relief: (1) invasion of privacy under Article I, Section 1 of the California Constitution; (2) intrusion upon seclusion under California common law; (3) violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630 et seq.; (4) violation of the Electronic Communications Privacy Act ("ECPA" or "Wiretap Act"), 18 U.S.C. § 2510 et seq.; (5) unjust enrichment; and (6) "declaratory judgment" that LiveRamp wrongfully accessed, collected, stored, disclosed, sold, and otherwise improperly used Plaintiffs' personal information and injunctive relief.

II. JURISDICTION

The Court has federal question jurisdiction over Plaintiffs' Wiretap Act claim pursuant to 28 U.S.C. § 1331 and supplemental jurisdiction over their state law claims pursuant to 28 U.S.C. § 1367(a). This Court also has jurisdiction under 28 U.S.C. § 1332(d).

III. LEGAL STANDARD

A complaint must contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). "Dismissal under Rule 12(b)(6) is appropriate only where the complaint lacks a cognizable legal theory or sufficient facts to support a cognizable legal theory." *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008). A complaint need not contain detailed factual allegations, but facts pleaded by a

plaintiff "must be enough to raise a right to relief above the speculative level." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (internal quotation marks and citation omitted). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* The Court must "accept all factual allegations in the complaint as true and construe the pleadings in the light most favorable to the nonmoving party." *Knievel*, 393 F.3d at 1072. However, the Court is not "required to accept as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (internal quotation marks and citation omitted).

IV. REQUEST FOR JUDICIAL NOTICE

"As a general rule, [courts] 'may not consider any material beyond the pleadings in ruling on a Rule 12(b)(6) motion.'" *United States v. Corinthian Colleges*, 655 F.3d 984, 998 (9th Cir. 2011) (quoting *Lee v. City of Los Angeles*, 250 F.3d 668, 688 (9th Cir. 2001)). "When 'matters outside the pleading are presented to and not excluded by the court,' the 12(b)(6) motion converts into a motion for summary judgment under Rule 56," unless those matters satisfy the "incorporation-by-reference doctrine" or the standard for "judicial notice under Federal Rule of Evidence 201." *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 998 (9th Cir. 2018) (quoting Fed. R. Civ. P. 12(d)). The Ninth Circuit has expressed concern with the practice of "exploiting these procedures improperly to defeat what would otherwise constitute adequately stated claims at the pleading stage." *Id.* The Ninth Circuit also cautioned that "[i]f defendants are permitted to present their own version of the facts at the pleading stage—and district courts accept those facts as uncontroverted and true—it becomes near impossible for even the most aggrieved plaintiff to demonstrate a sufficiently 'plausible' claim for relief." *Id.* at 999.

"Judicial notice under Rule 201 permits a court to notice an adjudicative fact if it is 'not subject to reasonable dispute,'" i.e., the fact "is 'generally known,' or 'can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned.'" *Id.* (quoting

Fed. R. Evid. 201(b)). "Unlike rule-established judicial notice, incorporation-by-reference is a judicially created doctrine that treats certain documents as though they are part of the complaint itself." *Id.* at 1002. Documents "may be incorporated by reference into a complaint if the plaintiff refers extensively to the document or the document forms the basis of the plaintiff's claim," *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003), and "the documents' authenticity . . . is not contested," *Lee*, 250 F.3d at 688 (alteration in original) (quotation marks and citation omitted). "[T]he mere mention of the existence of a document is insufficient to incorporate the contents of a document." *Coto Settlement v. Eisenberg*, 593 F.3d 1031, 1038 (9th Cir. 2010).

LiveRamp requests that the Court take judicial notice of four documents: (1) a copy of California Assembly Bill 929, Committee Report, from the 2015-2016 Regular Legislative Session, dated June 15, 2015; (2) a copy of Proposition 24, The California Privacy Rights Act of 2020 (codified at Cal. Civ. Code Ann. § 1798.100 (West 2025)); (3) a copy of California Assembly Bill 929, as adopted by the 2015-2016 Legislative Session on August 13, 2015; and (4) a copy of California Assembly Bill 929, Committee Report, from the 2015-2016 Regular Legislative Session, dated April 6, 2015. ECF No. 50.

Because courts regularly take judicial notice of government documents, and Plaintiffs do not dispute the authenticity of these documents, the Court takes judicial notice of the existence of these government documents, but not the truth of the matters asserted in those documents. *See Salas v. Gomez*, No. 14-CV-01676-JST, 2016 WL 3971206, at *5 (N.D. Cal. July 25, 2016); *see also In re Bare Escentuals, Inc. Sec. Lit.*, 745 F. Supp. 2d 1052, 1067 (N.D. Cal. 2010) (explaining that the court "may take judicial notice of the existence of unrelated court documents . . . it will not take judicial notice of such documents for the truth of the matter asserted therein").

V. DISCUSSION

A. Attribute Enrichment

As a preliminary matter, the parties disagree on whether the Court may dismiss only parts of a claim on a motion to dismiss. Defendants challenge Plaintiffs' invasion of privacy claims and claim for "declaratory judgment" only as far as they pertain to LiveRamp's RampID product and operation of the Data Marketplace—and not to the extent that those claims are based upon its

"Attribute Enrichment" feature. ECF No. 49 at 9. Plaintiffs respond that Defendants' failure to challenge the entirety of the claims at issue warrants denial of the motion to dismiss those claims. ECF No. 55 at 14–16. Plaintiffs further argue that even if partial dismissal is proper, it is inappropriate here because the factual allegations regarding Attribute Enrichment are "inextricably intertwined with LiveRamp's invasive conduct, and just one of a bundle of interrelated services within its surveillance infrastructure." *Id.* at 16 (citing ECF No. 32 ¶¶ 108–10).

The Court does not apply any categorical rule forbidding a defendant from targeting discrete factual allegations within a larger claim if that set of facts fails to state any plausible basis for relief. *See, e.g.*, *Staley v. Gilead Scis., Inc.*, No. 19-CV-02573-EMC, 2020 WL 5507555, at *11 (N.D. Cal. July 29, 2020) ("Often, a plaintiff asserts a single cause of action that is predicated on more than one liability theory, and a court eliminates one theory through a motion to dismiss."). But the Court agrees with Plaintiffs that the allegations about LiveRamp's Attribute Enrichment cannot be cleanly separated out because they are integral to understanding what LiveRamp does with its RampID profiles and how its Data Marketplace operates—both of which LiveRamp does contest as giving rise to claims for invasion of privacy.

Accordingly, the Court interprets Defendants' motion as challenging Plaintiffs' privacy claims and declaratory judgment "claim" only where those claims are based on LiveRamp's RampID and Data Marketplace features as independent bases of liability. But in so doing, the Court considers allegations regarding LiveRamp's Attribute Enrichment where relevant.

B. Privacy Claims

Because claims for intrusion upon seclusion and invasion of privacy under the California Constitution have "similar elements," courts "consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020) ("*Facebook Tracking*") (citing *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009)). When evaluating whether a reasonable expectation of privacy exists, "courts consider a variety of factors, including the customs, practices, and circumstances surrounding a defendant's particular activities." *Id.* (citing *Hill v. NCAA*, 7 Cal. 4th 1, 36 (1994)). The question is "whether a defendant

gained 'unwanted access to data by electronic or other covert means, in violation of the law or social norms.'" *Id.* (quoting *Hernandez*, 47 Cal. 4th at 286).

LiveRamp argues that Plaintiffs have not plausibly alleged that LiveRamp violated their reasonable expectation of privacy because they have not alleged that any of the specific data collected on them was sensitive. More specifically, it argues that its alleged compilation of offline data (names, addresses, emails) "is no different than maintaining a phone directory" and that the contact information it collects is not confidential. ECF No. 49 at 15. LiveRamp similarly argues that Plaintiffs do not have a reasonable expectation of privacy in their online activity—such as their browsing history and IP addresses—because Plaintiffs have not sufficiently alleged that there was anything sensitive captured in their online activity. *Id.* at 16–17.

Plaintiffs respond that "the aggregation of large quantities of data can itself constitute a violation of the reasonable expectation of privacy, even when individual data points might not otherwise be protectable." ECF No. 55 at 17. They argue that when examining both the sensitivity of the data collected and the manner in which that data was collected, LiveRamp's alleged conduct violates social norms and Plaintiffs' reasonable expectation of privacy. *Id.* (citing *Facebook Tracking*, 956 F.3d at 603). Plaintiffs' argument places great weight on *Facebook Tracking*.

In *Facebook Tracking*, the Ninth Circuit considered whether the plaintiffs had adequately alleged claims that Facebook was liable for violations of their privacy rights when it tracked—for the purpose of selling that information to third parties—their browsing histories even after they had logged out of their Facebook accounts. 956 F.3d at 596, 607–08. The Ninth Circuit ultimately held that "the allegations that Facebook allegedly compiled highly personalized profiles from sensitive browsing histories and habits prevent us from concluding that the Plaintiffs have no reasonable expectation of privacy." *Id.* at 604.

LiveRamp attempts to distinguish *Facebook Tracking* from the case at hand by arguing that: (1) unlike in *Facebook Tracking*, there is no allegation here that LiveRamp or its customers affirmatively represented that they would not be collecting Plaintiffs' data; (2) *Facebook Tracking* involved a larger amount of data from a greater number of sources than alleged here; (3) the

"nature" of the data collected and aggregated in *Facebook Tracking* was more sensitive than the data allegedly collected here; and (4) the pseudonymized nature of the RampID distinguishes it from the personal Facebook profiles, which correlated collected data with personal Facebook profiles. *See* ECF No. 49 at 18–20. The Court addresses these arguments in turn.

First, while the Ninth Circuit in *Facebook Tracking* found relevant to its analysis that Facebook had represented that it would not collect information on users when they were logged out but did so nonetheless, it did not hold that such misrepresentations are required to establish a reasonable expectation of privacy. *See Facebook Tracking*, 956 F.3d at 602–04. Instead, it explained that the critical inquiry concerns the sensitivity of the data collected and the manner in which it was collected—of which Facebook's misleading privacy policies were only one example. *Id.* at 604. And the Court similarly finds unpersuasive on this point LiveRamp's contention that it publicly discloses its data collection practices or that other websites mentioned in the complaint, like CVS, disclose their data collection practices in their privacy policies. As Plaintiffs allege, they were not aware of LiveRamp's conduct at all, *see* ECF No. 32 ¶¶ 149–63, so LiveRamp's disclosures have no effect on their reasonable expectations of privacy. *See Hart v. TWC Prod. & Tech. LLC*, 526 F. Supp. 3d 592, 601 (N.D. Cal. 2021) ("[T]he mere existence of a privacy policy is not dispositive because users might lack actual or constructive notice of the policy.") (citing *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1073–74 (N.D. Cal. 2016)). As for LiveRamp's assertion that CVS's privacy policies disclose the data collection practices referenced in the FAC, the Court does not consider facts not properly before it at the motion to dismiss stage. *See Arpin v. Santa Clara Valley Transp. Agency*, 261 F.3d 912, 925 (9th Cir. 2001).

Second, the Court sees no relevance to whether the amount of data LiveRamp allegedly collects is less than that involved in *Facebook Tracking*, i.e., hundreds or tens of thousands of websites rather than millions of websites. *Facebook Tracking*'s principal concern was the capacity of new technologies to track and compile both online and offline activity to "provide access to a category of information otherwise unknowable and 'implicate privacy concerns in a manner different from traditional intrusions." *See Facebook Tracking*, 956 F.3d at 603 (internal quotations omitted). And LiveRamp provided no reason to conclude that the privacy concerns

articulated in *Facebook Tracking* exist only when data is aggregated at the largest conceivable scale. Drawing all reasonable inferences in Plaintiffs' favor, the Court finds that the tracking of individuals' activity across thousands of websites, combined with extensive offline records gathered over decades, to generate uniquely identifying profiles on those individuals is sufficient to allege intrusion into privacy.

Third, the Ninth Circuit has already rejected Facebook's similar argument that in order to show a reasonable expectation of privacy, a plaintiff must "identify specific, sensitive information that Facebook collected" and that a "more general allegation that Facebook acquired an enormous amount of individualized data is insufficient." *Facebook Tracking*, 956 F.3d at 603 (internal quotation marks omitted). Instead, as the Ninth Circuit explained, the relevant question is "whether the data itself is sensitive and whether the manner it was collected . . . violates social norms." *Id.* Here, as in *Facebook Tracking*, Plaintiffs have alleged the comprehensive aggregation of data that reveals a person's internet activity with specificity such that the RampID profiles allow others to determine an individual's personal interests, searches, and habits on third-party websites. *See* ECF No. 32 ¶ 7 ("LiveRamp makes or has made available for sale segments of people with cancer, union members, Muslims, Jewish people, African Americans, poor people, payday loan prospects, online gamblers, unemployed individuals who were 'seen at clinics/hospitals' and users of the LGBT dating app Grindr."). Like in *Facebook Tracking*, the Court here cannot conclude at the pleading stage that Plaintiffs had no reasonable expectation of privacy in the information that LiveRamp compiled across hundreds to thousands of disparate online and offline sources and then sold to third parties without their knowledge or consent.

Fourth, the Court does not find LiveRamp's "pseudonymization" argument persuasive, as Plaintiffs allege that the Attribute Enrichment feature allows any of LiveRamp's customers to seek any "segment" information associated with an individual by providing the individual's name, physical address, or email address—effectively rendering any anonymity functionally meaningless. *See* ECF No. 32 ¶ 108.

Furthermore, a court in this district has applied *Facebook Tracking* to allow claims for invasion of privacy to proceed in almost identical circumstances. In *Katz-Lacabe v. Oracle*

America Inc., the plaintiffs brought suit against Oracle based on its extensive data brokering business—primarily challenging Oracle's identity resolution product and its data marketplace, which was "allegedly one of the world's largest commercial data exchanges." *Katz-Lacabe v. Oracle Am., Inc.*, 668 F. Supp. 3d 928, 935 (N.D. Cal. 2023). The court there applied *Facebook Tracking* to find that the plaintiffs' allegation that "Oracle's accumulation of a 'vast repository of personal data,'—from compiling Plaintiffs' browsing activity, online communications, *and* offline activity" sufficiently stated a claim that Oracle violated their reasonable expectation of privacy. *Id.* at 942. The court further reasoned that although it was—based on plaintiffs' generalized allegations—a "close question as to whether Oracle plausibly did collect and aggregate information to reveal" insights on "sensitive health and personal safety information," "viewing the allegations in the light most favorable to Plaintiffs, such allegations of data collection would go well beyond the routine commercial behavior of collecting contact information for sending advertisements." *Id.* (internal citations and quotation marks omitted).

Here, Plaintiffs argue that "LiveRamp provides functionally identical services to Oracle's: tracking and identity resolution to create persistent identifiers linked to comprehensive behavioral profiles, and a data marketplace enabling the sale of sensitive personal information." ECF No. 55 at 21. The court thus agrees with the analysis in *Katz-Lacabe* and is, for the reasons discussed above, unpersuaded by LiveRamp's attempt to distinguish the case based purely on an alleged difference in the scale of data collection. *See* ECF No. 49 at 20; ECF No. 56 at 12.

The Court also rejects LiveRamp's invitation to determine that the alleged intrusion wasn't offensive or serious. "Under California law, courts must be reluctant to reach a conclusion at the pleading stage about how offensive or serious the privacy intrusion is." *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 797 (N.D. Cal. 2019). When determining whether an invasion is "highly offensive," courts consider "the degree and setting of the intrusion," as well as "the intruder's motives and objectives." *Hernandez*, 47 Cal. 4th at 287. Given the factually intensive nature of the inquiry, "[c]ourts are generally hesitant to decide claims of this nature at the pleading stage." *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 799. Only if the allegations "show no reasonable expectation of privacy or an insubstantial impact on

privacy interests" can the "question of [a serious or highly offensive] invasion [ ] be adjudicated as a matter of law." *Hill*, 7 Cal. 4th at 40. Plaintiffs have alleged enough in the FAC such that the Court cannot at this stage conclude as a matter of law that the alleged aggregation, synthesis, and sale of comprehensive online and offline data of individuals without their knowledge is not highly offensive. *See Katz-Lacabe*, 668 F. Supp. 3d at 942–43; *see also Facebook Tracking*, 956 F.3d at 606 ("The ultimate question of whether . . . [Defendants'] practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage.").[2]

Finally, the Court does not find that Section 230 of the Communications Decency Act, 47 U.S.C. 230(c)(1), applies here to bar Plaintiffs' claims regarding the Data Marketplace. "Section 230 of the Communications Decency Act ("CDA") 'immunizes providers of interactive computer services against liability arising from content created by third parties.'" Kimzey v. Yelp! Inc., 836 F.3d 1263, 1265 (9th Cir. 2016) (quoting Fair Hous. Council of San Fernando Valley v. Roommates.*c*om, LLC, 521 F.3d 1157, 1162 (9th Cir. 2008) (en banc)). Section 230(c)(1) of the CDA makes clear that it "only protects from liability (1) a provider or user of an interactive computer service (2) whom a plaintiff seeks to treat, under a state law cause of action, as a publisher or speaker (3) of information provided by another information content provider." Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1100–01 (9th Cir. 2009), *as amended* (Sept. 28, 2009). The first element is to be interpreted "expansively," Kimzey, 836 F.3d at 1268, and Plaintiffs do not dispute that LiveRamp is an internet service provider. However, LiveRamp fails to meet the second and third elements of the test.

With regard to the second element, Plaintiffs are not seeking to treat LiveRamp as a "publisher or speaker," given that they are not asking LiveRamp to "review[ ], edit[ ], and decid[e] whether to publish or withdraw from publication third-party content." *Barnes*, 570 F.3d at 1102. Instead, Plaintiffs are asking LiveRamp "to moderate *its own* content." *Brooks v. Thomson Reuters Corp.*, No. 21-CV-01418-EMC, 2021 WL 3621837, at *13 (N.D. Cal. Aug. 16, 2021) (emphasis in original).

[2] For the same reasons, the Court similarly rejects LiveRamp's argument that its conduct is not offensive or serious because it complies with California's privacy laws.

With regard to the third element, CDA immunity does not apply when the defendant contributes to or shapes the content at issue, effectively becoming an "information content provider." *Roommates.com, LLC*, 521 F.3d at 1167–68. Here, Plaintiffs allege that LiveRamp obtains personal data from a variety of third-party sources and builds comprehensive identity profiles of individuals, then sells those profiles on the Data Marketplace. *See, e.g.*, ECF No. 32 ¶ 128 (quoting LiveRamp as advertising that "LiveRamp can create custom segments specifically for a campaign or advertiser"); *id.* ¶ 114 ("LiveRamp knowingly and deliberately aggregates otherwise virtually unassociated information and transforms it into commodity that reveals detailed and sensitive data tied to individual people via its RampID identity graph system. LiveRamp then makes that data commercially available on its Data Marketplace."); *id.* ¶¶ 108–10 (alleging that through its Attribute Enrichment feature, LiveRamp "returns whatever 'demographics and psychographic data' have been requested as an attachment to the original customer file"). The Data Marketplace does not consist only of user-generated content; rather, LiveRamp "generates all the dossiers with Plaintiffs' personal information that is posted on the [Data Marketplace]." *Brooks*, 2021 WL 3621837, at *13. "In other words, [LiveRamp] *is* the 'information content provider' of the [Data Marketplace] dossiers because it is 'responsible, in whole or in part, for the creation or development of' those dossiers." *Id.* (quoting 47 U.S.C. § 230(f)(3) (emphasis in original); *see also Parisi v. Sinclair*, 774 F. Supp. 2d 310, 318 n.3 (D.D.C. 2011) (finding that where companies do more than just "provide[ ] the online marketplace where third-parties [can] list and sell goods to customers" and instead actually are "distributors" of the goods, they "cannot rely on CDA immunity as a defense to plaintiffs' distributor-based claims"). The cases cited by Defendant do not assist LiveRamp because in those cases defendants made no material contribution to the third-party content they were publishing. *E.g., Planet Green Cartridges, Inc. v. Amazon.com, Inc.*, No. CV 23-6647-JFW(KSX), 2023 WL 8943219, at *6 (C.D. Cal. Dec. 5, 2023), *aff'd*, No. 23-4434, 2025 WL 869209 (9th Cir. Mar. 20, 2025).

C. CIPA and Wiretap Act Claims

1. Wiretap Act

The Wiretap Act provides for civil penalties against any person who "intentionally

intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). The Wiretap Act is a one-party consent statute. 18 U.S.C. § 2511(2)(d); *see also In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1026 (N.D. Cal. 2014) ("[T]he consent of one party is a complete defense to a Wiretap Act claim.").

LiveRamp argues that Plaintiffs' Wiretap Act claim must be dismissed because Plaintiffs have "alleged only that the LiveRamp pixel operates on websites of LiveRamp clients who have chosen to enable it." ECF No. 49 at 27. Plaintiffs respond that any consent is nullified by the Act's crime-tort exception.[3] *See* 18 U.S.C. § 2511(2)(d) (stating that there is a Wiretap Act violation even with consent if the "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State").

The crux of the parties' disagreement on this claim thus centers on whether the crime-tort exception applies here. LiveRamp cites *Katz-Lacabe* for the proposition that the crime-tort exception only applies when '"the primary motivation or a determining factor in the interceptor's actions has been to injure plaintiffs tortiously' . . . [and not] where Defendant's 'purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money.'" *Katz-Lacabe*, 668 F. Supp. 3d at 945 (quoting *Rodriguez v. Google LLC*, No. 20-cv-04688-RS, 2021 WL 2026726, at *6 n.8 (N.D. Cal. May 21, 2021), which in turn cites *In re Google Inc. Gmail Litigation*, No. 13-MD-02430-LHK, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014)). *In re Google Inc. Gmail Litigation* in turn relied on the reasoning in *In re DoubleClick Inc. Privacy Litigation*, 154 F.Supp.2d 497, 518 (S.D.N.Y. 2001).

The Court has carefully reviewed the *DoubleClick* line of cases and respectfully disagrees with the reasoning contained in them. In *In re DoubleClick*, Judge Buchwald reasoned:

> DoubleClick's purpose has plainly not been to perpetuate torts on

[3] Plaintiffs also dispute in a footnote whether they carry the burden of alleging that LiveRamp's clients did not consent to the use of the LiveRamp pixel. ECF No. 55 at 29 n.10. Because the Court finds that successful assertion of the crime-tort exception negates any consent, it does not address whether LiveRamp's clients in fact consented to the alleged interception.

> millions of Internet users, but to make money by providing a valued service to commercial Web sites. If any of its practices ultimately prove tortious, then DoubleClick may be held liable for the resulting damage. However, a culpable mind does not accompany every tortious act. In light of the abundant evidence that DoubleClick's motivations have been licit and commercial and the utter lack of evidence that its intent has been tortious, we find as a matter of law that plaintiffs have failed to allege that DoubleClick has acted with a "tortious" purpose.

In re DoubleClick, 154 F. Supp. 2d at 519.

Unlike the *DoubleClick* court and the courts that have followed it, this Court is not persuaded that commercially exploiting unlawfully obtained information is "licit" merely because it is profitable. Put simply, committing a tort and seeking a profit are not mutually exclusive (if anything, the latter is often the reason for the former). Thus, if Plaintiffs ultimately prove that LiveRamp unlawfully intercepted, packaged, and sold personal information without consent at scale, that conduct will not be excused on the grounds that LiveRamp acted in pursuit of profit. Other cases have come to the same conclusion. *See, e.g.*, *R.S. v. Prime Healthcare Servs., Inc.*, No. 5:24-CV-00330-ODW (SPX), 2025 WL 103488, at *7 (C.D. Cal. Jan. 13, 2025) ("Under Prime Healthcare's reading, the ECPA would not prohibit a person from intercepting a communication with the intent to use that communication to blackmail so long as the ultimate reason for the blackmail was to make money. . . . Of course, this is often the end goal for blackmail. . . . Under Prime Healthcare's reading, blackmail would rarely, if ever, violate the ECPA. This cannot be the case."). As one other court explained, "it would be odd to exclude an otherwise criminal or tortious act solely because it was also motivated by financial gain. The existence of an underlying financial motivation does not mean that the act lacked a criminal or a tortious purpose. That's like saying that a bank robber's purpose was not to commit a crime—it was to make money." *Stein v. Edward-Elmhurst Health*, No. 23-CV-14515, 2025 WL 580556, at *6 (N.D. Ill. Feb. 21, 2025).

Accordingly, the Court declines to adopt any "bright-line rule insulating financial motives from the crime-tort exception." *Castillo v. Costco Wholesale Corp.*, No. 2:23-CV-01548-JHC, 2024 WL 4785136, at *6 (W.D. Wash. Nov. 14, 2024); *see also Stein*, No. 23-CV-14515, 2025 WL 580556, at *6 ("[T]he existence of a financial motivation is not a get-out-of-liability-free

card."). Because Plaintiffs have otherwise adequately alleged that LiveRamp intercepted their communications for the purpose of "associating their data with preexisting [identity] profiles" and then preparing that data for sale on LiveRamp's data marketplace—triggering the crime-tort exception and rendering consent an inapplicable defense—the Court declines to dismiss their Wiretap Act claim. *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1067 (N.D. Cal. 2021); *see also Planned Parenthood Fed'n of Am., Inc., v. Ctr. for Med. Progress*, 214 F. Supp. 3d 808, 828 (N.D. Cal. 2016).

2. CIPA § 631(a)

Section 631(a) creates four avenues for relief:

> (1) where a person "by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection ... with any telegraph or telephone wire, line, cable, or instrument";
>
> (2) where a person "willfully and without consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit";
>
> (3) where a person "uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained"; and
>
> (4) where a person "aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above."

Javier v. Assurance IQ, LLC, 649 F. Supp. 3d 891, 897 (N.D. Cal. 2023) (quoting Cal. Penal Code § 631).

Plaintiffs assert a claim against LiveRamp based on the second avenue—alleging that LiveRamp reads the personal information it intercepts through its ATS.js code on its client websites while that information is "in transit."

LiveRamp argues that Plaintiffs have not adequately alleged a violation of CIPA § 631(a) because the FAC at most describes the interception of communications—not any "reading" of their contents and not while those communications are "in transit." More specifically, LiveRamp argues that "Plaintiffs' own theory is that LiveRamp's software transmits URLs and other inputs *instantaneously* 'before the requested page is completely loaded on their devices', which is much

too fast to permit real-time review.'" ECF No. 49 at 29 (quoting ECF No. 32 ¶ 214). LiveRamp relies in large part on *Torres v. Prudential Fin., Inc.*, 2025 WL 1135088 (N.D. Cal. Apr. 17, 2025), where the court granted summary judgment for the defendant on plaintiff's Section 631(a) claim after finding that "there is no evidence in the record that [the defendant's employees] access communications while they are in transit" as opposed to accessing or analyzing those communications *after* they have been transmitted to the server. *Torres*, 2025 WL 1135088, at *5.

As *Torres* itself illustrates, however, whether communications are "read" in transit or only after storage is a fact-intensive question that depends on how the challenged technology and processes actually work—a question *Torres* decided only after a full evidentiary record at summary judgment. And Plaintiffs' FAC contains specific factual allegations that, if taken as true, plausibly allege real-time interception and contemporaneous reading within the meaning of § 631(a). For example, the FAC alleges that LiveRamp's "[e]vent listeners intercept communications while in transit, once user inputs are made but before the communications are received by the webpage." ECF No. 32 ¶ 79; *see also id.* ¶ 217 (alleging that LiveRamp uses "'event listeners' to detect specific types of contents of communications . . . and intercept those contents and *simultaneously* transmit them to LiveRamp."). Together with Plaintiffs' other allegations that LiveRamp's identity graph "connects all these identifying points of data into a single, non-anonymous 'identity profile' . . . in real time," *id.* ¶ 6, Plaintiffs have set forth a specific factual theory as to how LiveRamp incorporates—and thus reads—the intercepted content "in real time" to update its identity profiles before that content is "completely loaded" onto the requested page, *id.* ¶ 214. That distinguishes Plaintiffs' allegations from the conclusory allegations which courts have found do not plausibly state a claim because they merely "restate the pleading requirement of real time interception" without providing any "specific facts as to how or when the interception takes place." *Valenzuela v. Keurig Green Mountain, Inc.*, 674 F. Supp. 3d 751, 758–59 (N.D. Cal. 2023).

While LiveRamp may ultimately be able to show that it does not actually "read" any intercepted communications "in real time," that factual dispute is better left for summary judgment. Accordingly, Plaintiffs have plausibly stated a claim under Section 631(a). *See Hazel*

v. Prudential Fin., Inc., No. 22-CV-07465-CRB, 2023 WL 3933073, at *4 (N.D. Cal. June 9, 2023) (finding that the plaintiffs plausibly alleged "that TrustedForm recorded their actions on Prudential's website before their information was stored by Prudential" and that whether "that information was intercepted by TrustedForm before it was stored by Prudential as Plaintiffs allege, or vice versa, is a question for summary judgment").

3. CIPA § 638.51

Plaintiffs bring a claim under California Penal Code Section 638.51, which prohibits any person from using a "pen register" without a court order, based on LiveRamp's usage of "Client-Side Tags, Enhanced Client-Side Tags, and ATS.js JavaScript code and SDK functionality" that allegedly "record" "addressing or signaling information,"—such as IP addresses and electronic device identification numbers. ECF No. 32 ¶ 227.

LiveRamp argues that Plaintiffs has failed to state a claim under Section 638.51 of CIPA because that section applies only to telephones and so the technologies Plaintiffs identify do not qualify as pen registers. To support its argument, LiveRamp cites (1) other statutory provisions enacted at the same time as the pen register prohibition, such as Sections 638.52(c) and 638.52(d), which do specifically discuss the use of pen registers in relation to a telephone number or telephone line; (2) the section's legislative history, in which the author of the bill and a committee report described pen registers in relation to the recording of telephone calls; and (3) a California Superior Court case holding that "pen register" refers to devices or processes that are used to record or decode information only from telephone numbers and not internet communications, *Sanchez v. Cars.com Inc.*, 2025 WL 487194, at *3 (Cal. Super. Jan. 27, 2025). ECF No. 49 at 29–32.

LiveRamp's first two citations actually undermine its arguments. Section 638.50 defines a "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication"—without limiting its application to telephones. Cal. Penal Code § 638.50(b). By contrast, other sections of CIPA specifically *do* include language regarding telephones. *See, e.g.*, Cal. Penal Code §§ 631(a)

(applying the statute to any "telegraph or telephone wire, line, cable, or instrument"); 632.7 (applying the statute to "a communication transmitted between two cellular radio telephones, a cellular radio telephone and a landline telephone, two cordless telephones, a cordless telephone and a landline telephone, or a cordless telephone and a cellular radio telephone"). Thus, if the drafters of Section 638.50 intended for "pen register" to be limited to telephone technologies, they knew how to say so. Accordingly, other federal courts have interpreted the plain language of Section 638.50 expansively to find that "pen registers" includes data collection tools beyond those the record information from telephones. In *Greenley v. Kochava, Inc.*, the court explained:

> Moreover, the Court cannot ignore the expansive language in the California Legislature's chosen definition. The definition is specific as to the type of data a pen register collects—"dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted," but it is vague and inclusive as to the form of the collection tool—"a device or process." *See* Cal. Penal Code § 538.50(b). This indicates courts should focus less on the form of the data collector and more on the result. Thus, the Court applies the plain meaning of a "process" to the statute. A process can take many forms. Surely among them is software that identifies consumers, gathers data, and correlates that data through unique "fingerprinting." (Am. Compl. ¶¶ 67, 74.) Thus, the Court rejects the contention that a private company's surreptitiously embedded software installed in a telephone cannot constitute a "pen register."

Greenley v. Kochava, Inc., 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023); *see also Mirmalek v. Los Angeles Times Commc'ns LLC*, No. 24-CV-01797-CRB, 2024 WL 5102709, at *3–4 (N.D. Cal. Dec. 12, 2024) (citing *Greenley* to reject the argument that CIPA's pen register definition applies only to telephone technology and to hold that internet browser trackers can constitute pen registers).

LiveRamp also argues that "[i]f there was any doubt as to the reach of this provision, the rule of lenity requires the doubt to be resolved in favor of Defendants." ECF No. 49 at 31. The Court sees no role for that rule here. "The rule of lenity applies to criminal and punitive statutes and requires ambiguities to be resolved in favor of the defendant." *Sec. & Exch. Comm'n v. Bardman*, 231 F. Supp. 3d 442, 447 n.6 (N.D. Cal. 2017) (citing *Fed. Election Comm'n v. Arlen Spector '96*, 150 F. Supp. 2d 797 (E.D. Pa. 2001)). The "rule of lenity only applies if, after considering text, structure, history, and purpose, there remains a 'grievous ambiguity or

uncertainty in the statute.'" *Barber v. Thomas*, 560 U.S. 474, 488 (2010) (quoting *Muscarello v. United States*, 524 U.S. 125, 139 (1998)); *see also People v. Superior Ct. of Riverside Cnty.*, 81 Cal. App. 5th 851, 886 (2022) (explaining that the rule of lenity applies "only if the court can do no more than guess what the legislative body intended; there must be an egregious ambiguity and uncertainty to justify invoking the rule" (internal quotations omitted)). LiveRamp has argued for a certain interpretation of Section 638.50(b), but it has not established that any "grievous ambiguity" in the statute's express language.

Lastly, for the reasons discussed above, the Court respectfully disagrees with the California Superior Court's conclusion in *Sanchez*, which focused its analysis on the legislative history of the CIPA rather than on the expansive, plain language of Section 638.50. *See Sanchez*, 2025 WL 487194, at *3.

D. Unjust Enrichment

California cases disagree as to whether unjust enrichment is a standalone claim. Some think it is. *E.g.*, *Pro. Tax Appeal v. Kennedy-Wilson Holdings, Inc.*, 29 Cal. App. 5th 230, 238 (2018) ("The elements of a cause of action for unjust enrichment are simply stated as receipt of a benefit and unjust retention of the benefit at the expense of another.") (citations and quotation marks omitted)). Others think not. *Hill v. Roll Int'l. Corp.*, 195 Cal. App. 4th 1295, 1307 (2011) ("Unjust enrichment is not a cause of action, just a restitution claim."); *City of Oakland v. Oakland Raiders*, 83 Cal. App. 5th 458, 477–78 (2022) ("There is no cause of action in California labeled 'unjust enrichment.'"). "When a plaintiff alleges unjust enrichment, a court may 'construe the cause of action as a quasi-contract claim seeking restitution." *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015) (quoting *Rutherford Holdings, LLC v. Plaza Del Rey*, 223 Cal. App. 4th 221, 231 (2014)).

Regardless of whether the claim is labelled unjust enrichment or restitution, a plaintiff must allege the same two elements: "receipt of a benefit and unjust retention of the benefit at the expense of another." *Lectrodryer v. SeoulBank*, 77 Cal. App. 4th 723, 726 (2000); *Pro. Tax Appeal*, 29 Cal. App. 5th at 238 ("Generally, one who is unjustly enriched at the expense of another is required to make restitution."). "The benefit that is the basis of a restitution claim may

take any form, direct or indirect." *Pro. Tax Appeal*, 29 Cal. App. 5th at 238 (citing Restatement (Third) of Restitution and Unjust Enrichment § 1, com. (Am. L. Inst. 2011)). "The fact that one person benefits another is not, by itself, sufficient to require restitution. The person receiving the benefit is required to make restitution only if the circumstances are such that, as between the two individuals, it is *unjust* for the person to retain it." *Welborne v. Ryman-Carroll Found.*, 22 Cal. App. 5th 719, 725 (2018) (emphasis in original) (citation omitted).

LiveRamp argues that Plaintiffs have not adequately pleaded a claim for unjust enrichment—seizing upon this Court's prior language explaining that "restitution generally requires 'that a defendant has been *unjustly* conferred a benefit 'through mistake, fraud, coercion, or request.'" *Russell v. Walmart, Inc.*, 680 F. Supp. 3d 1130, 1133 (N.D. Cal. 2023) (quoting *Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015)) (emphasis added in original). But the Court's emphasis in *Russell* was on whether retention of the benefit would be *unjust*—not on identifying "mistake, fraud, coercion, or request" as the only possible ways in which such retention could be unjust.

Here, Plaintiffs have alleged that LiveRamp has "unjustly profited from tracking, disclosing, and profiting from Plaintiffs and U.S. Class members' internet activity and real-world activity to third parties without [their] knowledge or consent," conferring benefits "at the expense" of their privacy rights. ECF No. 32 ¶¶ 259–76. Because the FAC contains detailed factual allegations as to how LiveRamp has violated Plaintiffs' privacy rights to create a "surveillance ecosystem" at the heart of its revenue generation without their consent, Plaintiffs have sufficiently stated a claim for unjust enrichment. *See Hart v. TWC Prod. & Tech. LLC*, 526 F. Supp. 3d 592, 605 (N.D. Cal. 2021) ("Hart has sufficiently pleaded a claim by alleging that TWC unjustly benefited from the use of his location data."); *Katz-Lacabe*, 2023 WL 6466195, at *6 (allowing the plaintiffs to proceed with their unjust enrichment claim based on allegations that Oracle collected and sold information relating to their browsing activity and real-world location information—all without their consent or knowledge).

E. Claim for Declaratory Judgment

Plaintiffs' sixth cause of action is styled as "declaratory judgment that LiveRamp

wrongfully accessed, collected, stored, disclosed, sold, and otherwise improperly used plaintiffs' personal information and injunctive relief." ECF No. 32 at 87. Declaratory relief, however,w is a remedy and not a standalone cause of action. *See Doe 1 v. GitHub, Inc.*, 672 F. Supp. 3d 837, 861 (N.D. Cal. 2023); *see also Winecup Gamble, Inc. v. Gordon Ranch, LP*, No. 3:17-CV-00163-ART-CSD, 2023 WL 2308416, at *5 (D. Nev. Mar. 1, 2023) ("Although the Court is not aware of a case from the Supreme Court of the United States or the Ninth Circuit clearly establishing that there is no standalone cause of action under the federal [Declaratory Judgment] Act, district courts appear to have decided with near uniformity that there is no standalone cause of action under the federal Act."). Plaintiffs' "cause of action" for declaratory and injunctive relief is more properly considered part of their prayer for relief. Accordingly, the Court dismisses with prejudice Plaintiffs' sixth cause of action but notes that they may still seek declaratory and injunctive relief should they prevail on their claims. *See Sowinski v. Wells Fargo Bank, N.A.*, No. 11-6431-SC, 2012 WL 5904711, at *1 (N.D. Cal. Nov. 26, 2012).

CONCLUSION

For the reasons above, Plaintiffs' sixth cause of action for a declaratory judgment is dismissed without leave to amend, and Defendants' motion to dismiss is denied as to the remainder of the claims.

IT IS SO ORDERED.

Dated: July 18, 2025

JON S. TIGAR
United States District Judge